

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-134547

(43)Date of publication of application : 23.05.1995

(51)Int.Cl. G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 05-281295

(71)Applicant : HITACHI MAXELL LTD

(22)Date of filing : 10.11.1993

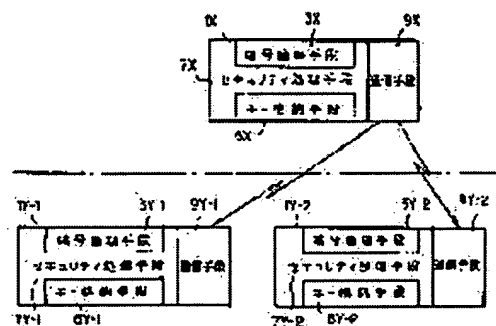
(72)Inventor : NAKAMURA TAKASHI

(54) INFORMATION TRANSFER SYSTEM AND CIPHER PROCESSOR USED THEREIN

(57)Abstract:

PURPOSE: To provide the information transfer system having high confidentiality.

CONSTITUTION: This information transfer system transfers information between at least a first terminal equipment 1X and a second terminal equipment 1Y and includes the following processing stages. A common key common between information users is formed by the first terminal equipment 1X. The common key is ciphered by the discrete keys discretely set for every information user in the first terminal equipment 1X to form discrete work keys. These work keys are transferred to the second terminal equipment 1Y where the transferred work keys described above are decoded by using the discrete keys possessed by the second terminal equipment 1Y to form the common key. The information to be transferred is ciphered by the common key to form the ciphered information. The ciphered information is transferred from the first terminal equipment 1X or the second terminal equipment 1Y to the other terminal device and the ciphered information transferred in such a manner is decoded to the original information by using the common key.



LEGAL STATUS

[Date of request for examination] 18.10.2000

[Date of sending the examiner's decision of rejection] 06.04.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-134547

(43) 公開日 平成7年(1995)5月23日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00		9364-5L		
H 0 4 L 9/06				
9/14				
			H 0 4 L 9/02	Z
			審査請求 未請求 請求項の数20	O L (全 13 頁)

(21) 出願番号 特願平5-281295

(22) 出願日 平成5年(1993)11月10日

(71) 出願人 000005810

日立マクセル株式会社

大阪府茨木市丑寅1丁目1番88号

(72) 発明者 中村 ▲昂▼

大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内

(74) 代理人 弁理士 武 顕次郎

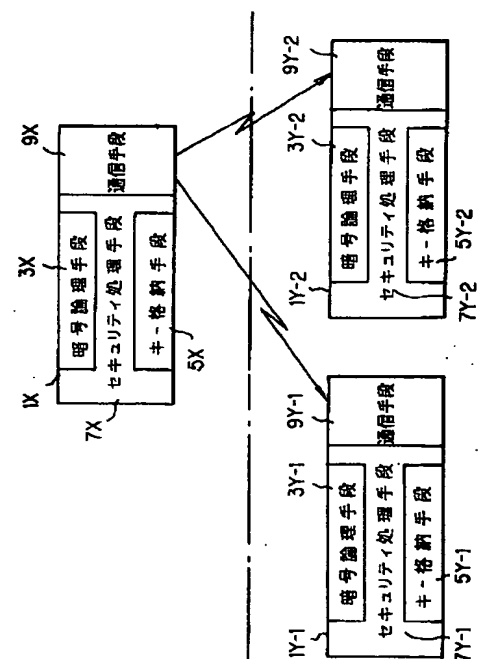
(54) 【発明の名称】 情報の受渡しシステムならびにそれに用いる暗号処理装置

(57) 【要約】

【目的】 機密性の高い情報の受渡しシステムを提供する。

【構成】 少なくとも第1の端末装置1Xと第2の端末装置1Yとの間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする。前記第1の端末装置1Xで、情報の利用者間で共通する共通キーを生成し、その第1の端末装置1Xにおいて、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、そのワークキーを前記第2の端末装置1Yに渡し、第2の端末装置1Yが有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、第1の端末装置1Xまたは第2の端末装置1Yから、他方の端末装置へ暗号化された情報を渡し、その渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【図1】



1

【特許請求の範囲】

【請求項 1】 少なくとも第 1 の端末装置と第 2 の端末装置との間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする情報の受渡しシステム。前記第 1 の端末装置で、情報の利用者間で共通する共通キーを生成し、

その第 1 の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、

そのワークキーを前記第 2 の端末装置に渡し、第 2 の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、

第 1 の端末装置または第 2 の端末装置から、他方の端末装置へ暗号化された情報を渡し、

その渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【請求項 2】 少なくとも第 1 の端末装置と第 2 の端末装置と第 3 の端末装置の間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする情報の受渡しシステム。前記第 1 の端末装置で、情報の利用者間で共通する共通キーを生成し、その第 1 の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、

そのワークキーを前記第 2 の端末装置ならびに第 3 の端末装置にそれぞれ渡し、

第 2 の端末装置ならびに第 3 の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、

渡す情報を前記共通キーで暗号化して暗号化情報を生成し、

第 1 の端末装置、第 2 の端末装置、第 3 の端末装置の間で暗号化された情報を渡し、

その受渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【請求項 3】 請求項 1 または 2 記載において、前記個別キーを前記第 1 の端末装置で生成して、各個別キーを他の端末装置に渡すように構成されていることを特徴とする情報の受渡しシステム。

【請求項 4】 請求項 3 記載において、前記第 1 の端末装置から第 2 の端末装置ならびに第 3 の端末装置への個別キーとワークキーの受渡しが別ルートになっていることを特徴とする情報の受渡しシステム。

【請求項 5】 請求項 3 記載において、前記個別キーを先に渡し、その後にワークキーまたは（ならびに）暗号化情報を渡すように構成されていることを特徴とする情報の受渡しシステム。

【請求項 6】 請求項 1 または 2 記載において、前記ワ

2

ークキーと暗号化情報が同時に渡されるように構成されていることを特徴とする情報の受渡しシステム。

【請求項 7】 請求項 1 または 2 記載において、前記ワークキーと暗号化情報が時間的にずらして渡されるように構成されていることを特徴とする情報の受渡しシステム。

【請求項 8】 請求項 1 または 2 記載において、前記個別キーまたは（ならびに）共通キーが変更可能であることを特徴とする情報の受渡しシステム。

10 【請求項 9】 請求項 1 または 2 記載において、前記情報の種類によって分類される種別キーが前記共通キーに付加されていることを特徴とする情報の受渡しシステム。

【請求項 10】 請求項 1 または 2 記載において、前記共通キーの有効期限を示す期限キーが前記共通キーに付加されていることを特徴とする情報の受渡しシステム。

【請求項 11】 少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第 1 の端末装置と第 2 の端末装置とを備え、

前記第 1 の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、渡すオリジナルの情報を前記共通キーで暗号化して暗号化情報を生成する機能を有し、

前記第 2 の端末装置が固有の個別キーを有し、前記第 1 の端末装置からのワークキーを個別キーで復号化して共通キーを生成し、第 1 の端末装置からの暗号化情報を生成した共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有していることを特徴とする暗号処理装置。

【請求項 12】 少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第 1 の端末装置と第 2 の端末装置とを備え、

前記第 1 の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、第 2 の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有し、

前記第 2 の端末装置が固有の個別キーを有し、前記第 1 の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有していることを特徴とする暗号処理装置。

【請求項 13】 少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納

50

手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第 1 の端末装置と第 2 の端末装置と第 3 の端末装置とを備え、

前記第 1 の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成する機能を有し、

前記第 2 の端末装置が固有の個別キーを有し、前記第 1 の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有し、

前記第 3 の端末装置が固有の個別キーを有し、前記第 1 の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、第 2 の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有していることを特徴とする暗号処理装置。

【請求項 14】 請求項 11 ないし 13 記載のいずれかにおいて、前記端末装置が、キーならびに暗号化情報を送受信する通信手段を備えていることを特徴とする暗号処理装置。

【請求項 15】 請求項 11 ないし 13 記載のいずれかにおいて、前記端末装置が装置本体とその装置本体に対して着脱可能な携帯用のキー格納部材とから構成され、少なくともそのキー格納部材にキーを格納するキー格納手段が、前記装置本体にキー読取手段が、それぞれ設けられていることを特徴とする暗号処理装置。

【請求項 16】 請求項 15 記載において、前記キー格納部材を装置本体に装着することにより、キー格納部材に格納されているキーを読み取るキー読取手段が装置本体に設けられていることを特徴とする暗号処理装置。

【請求項 17】 請求項 15 記載において、前記キー格納部材にキーの読み取りアクセスを保護するキー照合手段が設けられていることを特徴とする暗号処理装置。

【請求項 18】 請求項 15 記載において、前記キー格納部材に装置本体が暗号処理手段と、キー読取手段と、セキュリティ処理手段と、通信手段を有し、前記着脱部材がキー格納手段と、キー照合手段と、通信手段を有していることを特徴とする暗号処理装置。

【請求項 19】 請求項 15 記載において、1 つの装置本体に対して 2 つ以上のキー格納部材を有し、各キー格納部材に格納されている個別キーの内容が異なっていることを特徴とする暗号処理装置。

【請求項 20】 請求項 11 ないし 13 記載のいずれかにおいて、前記端末装置が信号用アダプタに内蔵されていることを特徴とする暗号処理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、機密保護を施した情報

の受渡しシステムならびにそれに用いる暗号処理装置に係り、さらに詳しくは、ソフトウェアの不正コピー防止が図れる機密性の高い情報の受渡しシステムとそれに用いる暗号処理装置に関するものである。

【0002】

【従来の技術】 従来、ソフトウェアのコピー防止については種々提案されているが、実際にはソフトウェアのセットアップ用ソフトでの使用回数のチェック、記憶装置の通常利用しないエリアのコードを該ソフトウェアの実行時に参照する等の簡単な方法が実用化されているに過ぎない。

【0003】

【発明が解決しようとする課題】 しかし、前述のようにソフトウェアのセットアップ回数のチェックやコードの参照などでは、機密の防止が不充分であった。

【0004】 特別の暗号処理装置を用いるものに、購入者自身がコピー防止希望時に自身のパスワードを該ソフトウェアに付加する方法もあったが、この方法は販売者又はレンタル会社が用いる方式には適用できず、複数種類のソフトに共通となるか、暗号処理装置をソフト毎に用意したり、差換えなければならないという不便があった。

【0005】 又、ネットワークを利用して送受信する情報の暗号化に関しては、パソコンやワークステーションにキーなどを格納して暗号化する方法があるが、これらの装置のキーを参照することは、第 3 者にとって比較的容易であり、機密防止の点では弱いものであった。

【0006】 今後、無線 LAN などの普及により、情報が無制限に近い領域に配布されとなると、高機密な暗号化方式、つまり、専用の暗号処理装置が必須となる。

【0007】 さらに、放送分野のペーパ TV（有料放送）では、放送情報の暗号化（スクランブル）が行なわれている。この方法は、視聴者は見たい番組を放送局に予め連絡し、自分の ID の入ったカード等を受信用デコーダに挿入し、放送局側に申出のカード ID かデコーダ番号を照合し、合致していれば所定の解読キーで復号化する方法である。

【0008】 従って、放送情報の中に、申出の ID かデコーダ番号かの識別のための情報を含める必要がある。

又、暗号化に用いるキーが、利用者毎の個別キーや番組（ないしは情報）毎の種別キーを含めて用いない為、これらを用いた暗号化キーの配布は必要ないが、固定的なキーによるので、不正解読の機会が多い。これを補完するためデコーダ内で、予め放送側と約束した一定のルールで、一定時間毎にキーを変化をさせる必要があった。

【0009】 本発明の目的は、前述したような、ソフト不正コピー防止が購入者に限定されたり、ネットワーク上の通信における機密の解読が容易であったり、放送においては申出者の識別情報を付加しなければならないなどの欠点を有効に解消し、機密性の高い情報の受渡しシ

システムならびにそれに用いる暗号処理装置を提供するにある。

【0010】

【課題を解決するための手段】前記目的を達成するため、第1の本発明は、少なくとも第1の端末装置と第2の端末装置との間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする。

【0011】前記第1の端末装置で、情報の利用者間で共通する共通キーを生成し、その第1の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、そのワークキーを前記第2の端末装置に渡し、第2の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、第1の端末装置または第2の端末装置から、他方の端末装置へ暗号化された情報を渡し、その渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【0012】前記目的を達成するため、第2の本発明は、少なくとも第1の端末装置と第2の端末装置と第3の端末装置の間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする。

【0013】前記第1の端末装置で、情報の利用者間で共通する共通キーを生成し、その第1の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、そのワークキーを前記第2の端末装置ならびに第3の端末装置にそれぞれ渡し、第2の端末装置ならびに第3の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、第1の端末装置、第2の端末装置、第3の端末装置の間で暗号化された情報を渡し、その受渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【0014】前記目的を達成するため、第3の本発明は、少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第1の端末装置と第2の端末装置とを備えている。

【0015】そして前記第1の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、渡すオリジナルの情報を前記共通キーで暗号化して暗号化情報を生成する機能を有し、前記第2の端末装置が固有の個別キーを有し、前記第1の端末装置からのワークキーを個別キーで復号化して共通キーを生成し、第1の端末装置

置からの暗号化情報を生成した共通キーで復号化してオリジナルの情報の情報に相当する情報を生成する機能を有していることを特徴とする。

【0016】前記目的を達成するため、第4の本発明は、少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第1の端末装置と第2の端末装置とを備えている。

【0017】そして前記第1の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、第2の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報の情報に相当する情報を生成する機能を有し、前記第2の端末装置が固有の個別キーを有し、前記第1の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有していることを特徴とする暗号処理装置。

【0018】前記目的を達成するため、第5の本発明は、少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第1の端末装置と第2の端末装置と第3の端末装置とを備えている。

【0019】そして前記第1の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成する機能を有し、前記第2の端末装置が固有の個別キーを有し、前記第1の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有し、前記第3の端末装置が固有の個別キーを有し、前記第1の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、第2の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報の情報に相当する情報を生成する機能を有していることを特徴とする。

【0020】

【作用】本発明は前述のような構成になっており、情報の暗号化は同一（共通）の値（内容）の共通キーRを使用しているから、情報に対しては共通キーRのみで一様に生産すればよいから処理が簡便である。

【0021】また、情報の利用者ごとに異なる値（内容）のワークキー（R）S_iを配布しているから、その解読は非常に困難である。

【0022】さらに情報の配布側と利用者側との間は、暗号化された情報（I）Rとワークキー（R）S_iしか流れないので、機密は高度に保たれるなどの特長を有している。

【0023】

【実施例】図1は、本発明の実施例に係る基本構成例を示すブロック図である。携帯できる暗号処理装置1 (SAM: Security Access Module) は、基本的には暗号論理手段3、キー格納手段5、セキュリティ処理手段7ならびに通信手段9から構成されている。

【0024】前記暗号論理手段3は、情報ならびにキーを暗号化するための各種の暗号論理が格納されている。暗号論理手段3として、例えばDES, RSA, Multi, FEAL, 0知識認証などがあるが、これらに限らず、暗号論理の全般のものが適用可能である。その実施方法も、ASICで専用回路を組むことも、既存ワンチップマイコンを用いることも可能である。

【0025】前記キー格納手段5には、後述するように共通キー、個別キー、ワークキー、種別キー、期限キーなどの各種キーが格納されるようになっている。

【0026】このキー格納手段5には、電源非供給時も消去されないEEPROM、フラッシュメモリ、EPROMなどが使用される。動作電源は、RS232Cの場合、パソコン本体から供給を受けることができる。JEIDA4.1インタフェースでは、内部に電池を保有することになる。

【0027】前記セキュリティ処理手段7は、キー格納手段5に格納されているキーの中から必要なキーを呼び出し、通信手段9を介して受け取られた情報を暗号論理手段3を用いて処理する機能を有している。

【0028】なお、キー格納手段5から必要なキーを呼び出すとき、呼び出すためのアクセスチェックとして、パスワードチェックすることもあるし、暗号を用いた相互認証することもある。

【0029】前記通信手段9は、外部との間で情報やキーなどの送受信を行なう機能を有している。この通信手段9は必ずしも1つであるとは限らず、例えばパソコンのRS232Cに直付けのコンタクトと他方外部の装置、例えばモデムなどと透過的(トランスピアレント)につなぐための出口としてのRS232Cのコンタクトの2つを持つこともある。JEIDA4.1インタフェースでパソコンとつなぎ、一方で、出口としてLANの10BASE-Tのコンタクト、ないしはモデムやモデムFAXを兼用の時は電話回線のスロットなどを持つこともある。

【0030】図1は情報を供給する側の暗号処理装置(端末装置)Xと、その情報を受ける側の暗号処理装置(端末装置)Yとに分けて図示しており、ここでは情報を供給する側の暗号処理装置が1個で、情報を受ける側の暗号処理装置Yが2個の例を示しているが、実際には暗号処理装置Yの数は多数であることが多い。またこの例では、暗号処理装置1の構成が全て同じ例が示されている。

【0031】前述のようにキー格納手段5には個別キーと共通キーが格納されており、図2はその個別キーと共通キーの関係をソフト不正コピー防止の用途を例にして示している図である。

【0032】この例は、ソフトデータの情報10を、第1の端末装置である暗号処理装置1 {SAM(1)} から第2の端末装置である暗号処理装置4 {SAM(2)} を介して伝送する例を示している。

【0033】携帯暗号処理装置1 {SAM(1)} が、情報10 {I(1)} の暗号化を図るべく共通キーRを生成する(同図のステップ①)。この生成は例えば図1の暗号論理手段3を用いて、乱数発生させれば容易に生成できる。ソフトデータの情報10は、同図に示すように例えばフロッピーディスクなどの情報記録媒体に格納されており、その情報10はリーダライターを介して読み出される(ステップ②)。

【0034】そしてこの共通キーRを用いて、前記情報10 {I(1)} を暗号化する(ステップ③)。この時の暗号化は、情報10の全体を暗号化してもよいし、一部分暗号化してもよいし、また情報に付加する付加情報(暗号化結果やハッシュトータル、ないしはパスワード、暗号化パスワード、パスワードチェックロジック等)のみを暗号化してもよい。

【0035】共通キーRは、情報10ごと(例えば:ソフトなら太郎とか、ロータス1, 2, 3, などの種類ごと)に変えることが好ましい。暗号化された情報

(I) Rは、オリジナルの情報I(1)とは区別し、暗号化情報(I) Rのみが暗号処理装置4 {SAM(2)} へ例えば通信手段などを使用して送られるか、製品に同梱されて配布され(ステップ④)、オリジナルの情報I(1)は配布されない。

【0036】次に共通キーRを個別キーSiで暗号化して、ワークキー(R) Siを生成する(ステップ⑤)。個別キーSiは、図1のキー格納手段5に予め格納されていると同時に、利用者の側にある携帯暗号装置4 {SAM(2)} にも予め付与されている。

【0037】SAM(1)1からSAM(2)4へワークキー(R) Siが、例えば通信手段9などを使用して送られるか、同梱されて渡される(ステップ⑥)。SAM(2)4側では、予め格納、保有している利用者自身の個別キーSiでワークキー(R) Siを復号化して、共通キーRを生成する(ステップ⑦)。この共通キーRで、さらに暗号化情報(I) Rを復号化して情報10 {I(1)} と同じソフトデータの情報14 {I(2)} を得て(ステップ⑧)、それをフロッピーディスクなどの情報記録媒体に格納することにより(ステップ⑨)、ソフトデータが不正にコピーされずに伝送される。ここでいう情報記録媒体は、例えばFD、MO、CD-ROM、テープ、カードなど各種の記録媒体が使用可能である。

【0038】前述のように利用者ごとに異なる値（内容）のワークキー（R） S_i を配布しているが（従ってこれを盗まれても、1人1人利用者毎に異なっているので、解読できない。）、暗号化は同一（共通）の値（内容）の共通キーRを使用しているから、情報に対しては共通キーRのみで一様に生産すればよい。配布側と利用者側との間は、暗号化された情報（I）Rとワークキー（R） S_i しか流れないので、機密は高度に保たれている。

【0039】ここでは説明を簡略化するため期限キーや種別キーの記述は省略したが、共通キーに期限キーや種別キーを加えて暗号化することもできる。すなわち、期限キーにより共通キーに有効期限を設け、その期限を経過した共通キーは使用できないシステムにすることができる。

【0040】また、伝送されるべき情報を例えば技術的、用途的、内容的、地理的など適宜な種類に分類し、各種類に対応させて種別キーを設定し、情報ごとにアクセス権を分けることができる。

【0041】前記図2では、情報の提供側と情報を受ける側が1対1の場合について説明したが、図3～8は情報を受ける側あるいは情報の提供側が複数ある場合を示している。

【0042】図3に示されているように、情報の提供側である1つのSAM（1）に対して情報を受ける側に2つのSAM（2）-A、SAM（2）-Bが設置されている。

【0043】そして前記SAM（1）にはSAM（2）-A用の個別キー S_{i-A} とSAM（2）-B用の個別キー S_{i-B} が予め生成されて格納されているとともに、SAM（2）-Aには個別キー S_{i-A} が、SAM（2）-Bには個別キー S_{i-B} が、それぞれ予め付与、保有されており、個別キー S_{i-A} と個別キー S_{i-B} は別の値（内容）を有する固有のものである。

【0044】まず、SAM（1）において共通キーRを生成する（ステップ①）。

【0045】そして共通キーRを前記個別キー S_{i-A} ならびに S_{i-B} で暗号化して、SAM（2）-A用のワークキー（R） S_{i-A} と、SAM（2）-B用のワークキー（R） S_{i-B} とを生成する（ステップ②）。このとき前述のように、共通キーRに期限キーあるいは（ならびに）種別キーなど他のキーを付加して暗号化することもできる。

【0046】生成したワークキー（R） S_{i-A} をSAM（2）-Aに、ワークキー（R） S_{i-B} をSAM（2）-Bにそれぞれ個別に送る（ステップ③）。

【0047】SAM（2）-AならびにSAM（2）-Bでは、送られたワークキー（R） S_{i-A} 、（R） S_{i-B} をそれぞれの個別キー S_{i-A} ならびに S_{i-B} を用いて復号化して共通キーRを生成する（ステップ

④）。以上のステップ①～④で、情報伝送のための準備が終了する。

【0048】次にSAM（1）において、伝送すべきオリジナル情報I（1）を前記共通キーRで暗号化して、暗号化情報（I）Rを生成する（ステップ⑤）。

【0049】この暗号化情報（I）Rを、送付先のSAM（2）-A、SAM（2）-Bにそれぞれ送る（ステップ⑥）。

【0050】SAM（2）-AならびにSAM（2）-Bでは、送られた暗号化情報（I）Rを前記共通キーRで復号化して、前記オリジナル情報I（1）に相当する情報I（2）を生成して（ステップ⑦）、情報の伝送を終了する。

【0051】図4は、情報伝送の変形例を示す図である。この例で図3に示す処理と相違する点は、SAM（1）でワークキー（R） S_i と暗号化情報（I）Rを生成した後、これらを同時にSAM（2）-AならびにSAM（2）-Bに送っている点である。なお、これらの情報を送るときには、同一の伝送ルートで送ってもよいし、例えばネットワークとファックスなど別の伝送ルートで送ってもよい。

【0052】図5は、情報伝送の他の変形例を示す図である。この例で図3に示す処理と相違する点は、SAM（2）-AとSAM（2）-Bが予め個別キー S_{i-A} 、 S_{i-B} を保有しているのではなく、情報を伝送する前にSAM（1）で個別キー S_{i-A} 、 S_{i-B} を生成してSAM（2）-AとSAM（2）-Bにそれぞれ送付する点である。SAM（1）での個別キー S_{i-A} 、 S_{i-B} の生成（更新、変更）は定期的であっても不定期的であってもよい。

【0053】図6は、情報伝送のさらに他の変形例を示す図である。この例の場合、それぞれ個別キー S_{i-A} 、 S_{i-B} を保有しており、SAM（1）で共通キーRを生成（ステップ①）し、ワークキー（R） S_i を生成（ステップ②）し、それをSAM（2）-AならびにSAM（2）-Bへ送付（ステップ③）して、SAM（2）-AならびにSAM（2）-Bで共通キーRを生成する（ステップ④）。

【0054】次にSAM（2）-A側が保有しているオリジナルの情報I（1）-AをSAM（2）-Aで共通キーRを使用して暗号化情報（I）R-Aを生成し、それをSAM（1）に送る（ステップ⑤）。

【0055】SAM（1）ではこの暗号化情報（I）R-Aを共通キーRで復号化してSAM（2）-A側の情報I（2）-Aを生成する（ステップ⑥）。

【0056】また、SAM（2）-B側が保有しているオリジナルの情報I（1）-BをSAM（2）-Bで共通キーRを使用して暗号化情報（I）R-Bを生成し、それをSAM（1）に送る（ステップ⑦）。

【0057】SAM（1）ではこの暗号化情報（I）R

ーBを共通キーRで復号化してSAM(2)ーB側の情報I(2)ーBを生成する(ステップ⑧)。

【0058】図7は、情報伝送のさらに他の変形例を示す図である。この例で前記図6の処理と相違する点は、ステップ⑤において暗号化情報(I)RーAをSAM(1)とSAM(2)ーBへ送り、SAM(1)ならびにSAM(2)ーBでこの暗号化情報(I)RーAを共通キーRで復号化してSAM(2)ーA側の情報I(2)ーAを生成する(ステップ⑥)点である。

【0059】図8は、ネットワーク上で本発明の暗号処理装置を使用した場合の構成例を示す図である。図中の30Aは情報を提供しようとするセキュリティサーバ側のパソコンで、暗号処理装置1が装着されている。30Bはクライアントー1側のパソコンで暗号処理装置4aが装着され、30Cはクライアントー2側のパソコンで暗号処理装置4bが装着されている。これらパソコン30A、30B、30Cは、LANや無線LANなどのネットワークシステム22によって相互に接続されている。

【0060】同図に示すように暗号処理装置1において共通キーRを生成(ステップ①)し、個別キーSiを用いてワークキー(R)Siを生成(ステップ②)し、パソコン30Aからネットワークシステム22を介してワークキー(R)SiーAを暗号処理装置4aに、ワークキー(R)SiーBを暗号処理装置4bに、それぞれ送信する(ステップ③)。

【0061】そして暗号処理装置4aではワークキー(R)SiーAを復号化して共通キーRを生成し、暗号処理装置4bではワークキー(R)SiーBを復号化して共通キーRを生成する(ステップ④)。

【0062】フロッピーディスクなどの情報記録媒体21をパソコン30Bに装着して、情報記録媒体21内のオリジナル情報Iを読み出し、それを共通キーRで暗号化して暗号化情報(I)Rを得る(ステップ⑤)。

【0063】この暗号化情報(I)Rをネットワークシステム22を介してパソコン30Cに送り(ステップ⑥)、暗号処理装置4bにおいて暗号化情報(I)Rを共通キーRで復号化してオリジナル情報Iに相当する情報を得る(ステップ⑦)ようなシステムになっている。

【0064】図9は図8で説明したパソコン30Bの側面図、図10はそのパソコン30Bに接続された暗号処理装置4aの処理動作を説明するためのフローチャートである。

【0065】図9に示されているように、パソコン30Bの後部にある通信用スロットにアダプタ20が接続され、それに暗号処理装置4aが内蔵されて、ネットワークシステム22用のケーブル23が付設されている。

【0066】次に暗号処理装置4aの処理動作について図10とともに説明する。まず、ステップ(S)1においてパソコン30B側から暗号処理装置4aにデータ伝

送の命令信号が入力される。S2では、その命令信号がアダプタ20の所定のピンNO.に送付されたかどうかのチェックがなされる。例えばアダプタ20に25本のピンがあり、そのうちのピンNO.1~6がセキュリティ処理に使用されるように設定されている。

【0067】命令信号が所定のピンNO.に送付されたことを確認すると、S3で復号化命令が出されたかどうか判断され、復号化命令が出されておれば次のS4に、そうでなければ後段のS6に進む。

【0068】S4で暗号処理装置4aに予め格納されている個別キーSiが呼び出され、パソコン30Aから送付されたワークキー(R)Siを復号化して共通キーRを生成し、S5でその共通キーRを暗号処理装置4aに格納して、終了レスポンスをパソコン30Bに返信する。

【0069】次に共通キーRの要求があったかどうか判断され、あると判断されると次のS7に、ないと判断されると後段のS9に進む。S7で共通キーRをレスポンスし、S8において共通キーRを用いてオリジナル情報Iを暗号化して、その暗号化情報(I)Rを受領者であるパソコン30Cにネットワークシステムを介して伝送する。

【0070】そしてS9で期限チェックなど暗号処理装置4aに関する命令等を全て処理した後、その暗号処理装置4aに対して暗号処理の機能をもたないで単にケーブルとして見做すスルー処理を行なう。

【0071】次に、実際の種別キーを存在させた場合のソフト販売またはレンタル時の運用について述べる。

【0072】図11は、図1に示したキー格納手段5をSAM1から分離させた場合を示しており、分離させることにより暗号処理装置SAM1がSAM1aとSAM1bに分かれる。

【0073】そして暗号処理装置SAM1aは同図に示すように、暗号論理手段3と、キー読取手段6と、セキュリティ処理手段7aと、通信手段9aとから主に構成されている。

【0074】一方、コンパクトな携帯用の暗号処理装置SAM1bは、キー格納手段5と、キー照合手段8と、通信手段9bとから主に構成されている。このSAM1bは、例えばシリアルメモリを持ったカードやペンシル型棒やコインなどであり、シリアルメモリはキー照合手段8によってパスワードチェックがOKなら中のキー情報を呼び出せる構成になっている。メモリはEEPROM、フラッシュメモリ、EPROMなどから構成されており、消去されず、電源も不要で、低コストの携帯キーとなる。

【0075】これに個別キーSiや期限キー、種別キーなど必要な各種キーを格納して、情報の入った記録媒体(FDやその他)と共に梱包され、販売時又はレンタル時に利用者に渡される。シリアルメモリに限らず、IC

カード、CPU付きペンやコイン、磁気カードなど各種のものが使用可能である。

【0076】利用者は、自分の許にあるSAM1aに、このSAM1bをセットしてキーの呼出しを行なう。もし、情報が複数の場合には各々にSAM1bが存在するので、SAM1aはこれらの複数のSAM1bをSAM1a内に一度だけ格納すればよい。このようにSAM1bを分けて、携帯可能に、又は暗号化情報(I)Rと同梱させることにより、高機密でコピーが不可能な状態になる。

【0077】ネットワーク上で情報のメールを高機密に行う場合、ワークステーションを一人で使用するのならSAM1bは無くても図1のSAM1で済み、ワークステーション1台を数人で使う時は、各自のSAM1bを使用時にSAM1aにセットすればよい。

【0078】ネットワークの場合、種別キーは無いが、期限キーはあってもよい。暗号化情報(I)Rは、ネットワークを介して伝送される。受信者は、予めセキュリティサーバから送られて来ているワークキー(R)Siを復号化して、共通キーRを得て、この共通キーRで暗号化情報(I)Rを復号化して情報を読むことになる。

【0079】個別キーSiや期限キー、暗号関数がワークステーションのハードディスクやメモリに格納されていると、盗聴されたり、ファイルがコピーされたりして、キーや暗号関数が盗まれる可能性が高い。しかし、本発明のSAM1を用いれば、これらは特別のハードの中にパスワード付きで内蔵され、呼出されるものはその一部の情報でそれしか外に出ないで、又、それを保有していないと動作しないので、機密性が非常に高い。

【0080】放送用のペーTVに用いる場合でも、ネットワークとほぼ同様で、各視聴者に予めワークキー(R)Siを配布し、個別キーSiを内蔵したICカード等にてワークキー(R)Siを復号化して、共通キーRを得る。その共通キーRで、暗号化情報(I)Rをオリジナル情報Iと同じ状態に復号化する。

【0081】図12～15は、各実施例に係る携帯暗号処理装置の外観図である。図12は、パソコンやWS30の通信スロット(RS232Cスロット)などの入出力装置に、暗号処理装置SAM1をアダプタの型で接続した場合を示している。

【0082】図中の20はアダプタで前記SAM1が組み込まれており、24は外向きのRS232Cスロット、又はLANインターフェース、又は電話接続コンタクト、25はパソコンやWS30のRS232Cスロットなどの入出力装置、30はパソコンのワークステーションである。なお、暗号処理装置SAM1の電源はパソコン30側から供給されるようになっている。

【0083】この実施例では前記アダプタ20を入出力装置25に接続することにより、本来のアダプタの機能の他に暗号処理機能が発揮でき、それも、利用者にとつ

ては、従来通りの入出力機能のみ意識で、暗号処理装置の機能は意識することなく、いわゆる透過的(トランスピアレント)に両機能が実現できるという特長を有している。

【0084】また、前記アダプタ20はLAN制御機能を内蔵し、外向きのインタフェース24として例えばLAN用の10-Base-T、10-Base-5、10-Base-10などの入出力ポート、RS232Cなどのシリアルポート、SCSI、IDEなどの既存のインタフェースポート、汎用の拡張ボードや専用の内蔵ボード、SIMMなどを利用することもできる。アダプタ20がファックスやモデムを兼用するときは出力口は電話接続用コンタクトとなり、無線LAN対応の受発信機でもよい。

【0085】図13は、暗号処理装置SAM1がSAM1aとSAM1bの2つに分かれ、SAM1b(SAM1b-1, SAM1b-2, ……SAM1b-n)が利用者ごとに異なった場合の外観図である。

【0086】SAM1aはアダプタ本体20aに内蔵され、SAM1b(SAM1b-1, SAM1b-2, ……SAM1b-n)は例えばペン型の着脱部材20bに内蔵され、この着脱部材20bはアダプタ本体20aに対して着脱可能になっている。この例では着脱部材20bは接続式のインタフェースを有しており、抜き出した時は胸のポケットにペン同様に収納できる。

【0087】また、アダプタ本体20aと着脱部材20bにそれぞれ信号送受信用ならびに給電用のコイルを設け、着脱部材20bをアダプタ本体20aに装着するかあるいは近づけることにより、両コイル間の磁気的結合を利用してSAM1aとSAM1bの間で信号の送受信と電力の供給を行うこともできる。

【0088】図14は、SAM1aとSAM1bがともにカード状になってに分かれる暗号処理装置の外観図である。

【0089】SAM1aはICカードなどからなるカード本体40に内蔵され、このカード本体40に対して着脱可能なサブカード41にSAM1b(携帯キー格納装置)が内蔵されされている。

【0090】カード本体40の上面側にはサブカード41が装着される凹部42が形成され、その凹部42内にはサブカード41との接続を図るための接点パネ43が設けられ、一方、サブカード41の下面には接点パネ43と接触する接点44が設置されている。

【0091】カード本体40の前部には、LANインターフェースやモデム、ファックスモデムのインターフェースなどからなる外向きインターフェース45が設けられている。また、カード本体40の後部には、JEIDA4, 1インターフェース46が設けられている。

【0092】この例では外部から機器の筐体を開ける作業をすることなく接続可能なICメモリカードの例を示

したが、これに限らずパソコンの筐体を開けてセットする、例えば汎用拡張ボードや機器ごとの専用内蔵ボードでも同様に実現できる。これらの場合は、パソコンの立上げ時の Boot セクタのコントロールまで可能なので、セキュリティ処理の実現がかなり容易になる。

【0093】個人別のキー格納媒体のリーダーライタの実装や LAN、モジュラーシックの出口の実装も該ボードで可能である。

【0094】図 15 は図 14 の変形例で、図 14 のサブカード 41 の代わりに例えばペン型などの着脱部材 47 が用いられ、それに SAM1b (携帯キー格納装置) が内蔵されされている。そしてこの着脱部材 47 が、カード本体 40 に対して着脱可能に装着されている。

【0095】本発明にかかる各種情報は、例えばフロッピーディスク、リードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、CD-I、MD、メモ리카ード、コンピュータテープ、VTRテープ、カセットテープなどの情報記録媒体に格納されている。

【0096】本発明の暗号処理装置の構成要素の 1 つ以上が、IC メモ리카ードにて実現され、JEIDA 4, 1 などの標準インタフェースにて実現できる。またその IC メモ리카ードが、前記キー格納部材の入出力装置となっており、JEIDA 4, 1 のインタフェースに IC メモ리카ードを挿入し、さらに、該 IC メモ리카ードにキー格納部材を接続して、一連の暗号処理を行うことができる。

【0097】また前記 IC メモ리카ードが、通信用のモデム (変復調装置)、ファクシミリ送受信機能、無線通信機能、ローカルエリアネットワークインタフェース機能、などのいずれか 1 つか、複数の機能を実装し、暗号処理機能のみならず他の機能も発揮できて、該 IC メモ리카ードには、JEIDA 4, 1、携帯キー格納装置の入出力インタフェースなどの他にモデム、FAX、無線通信、LAN などの入出力ポートをも具備することができる。

【0098】前記携帯用のキー格納部材が、中央処理装置 CPU を用いたマンチップマイコンによるもの、シリアルメモリによるもの、ASIC 論理機構によるもの、磁気媒体によるもの、光学的コードの読書によるもの、電磁波によるもの、ラジオ周波数等の電波によるものなどの中の 1 つ又は、複数の用いて実現することも可能である。

【0099】また IC メモ리카ードの代わりに、RS 232C のシリアルポートにケーブルレスにアタッチしたアダプタに本発明の暗号処理装置を内蔵し、該アダプタがパソコンと直接接続するポートの他に外部と接続するポートを有し、常時接続状態にすることもできる。

【0100】本発明の暗号処理機能のうち、暗号処理装置が接続されているパソコン、ワークステーション、インテリジェント電話などの本体の側で、情報の暗号化や

復号化を行ない、携帯暗号処理装置で、キーの暗号化、復号化およびキーの格納、生成、照合など行なうように機能分担させることも可能である。

【0101】本発明に係る情報が、ネットワーク、パソコン通信、BS や CS などの有料無料の衛星放送、地上波やケーブル TV、無線ネットワーク、電話網、無線電話網、アマチュア無線通信、などで送受信する情報、プログラム、データ、音声画像、などであり、送受の両方で、暗号化と復号化を行なうことによって、高機密に情報の受渡しや課金の処理を行なうことも可能である。

【0102】本発明による情報の暗号化、復号化は単に全ての情報の暗号化、復号化を指すのではなく、一部の情報を対象にするか、情報に付加するキーチェックモジュールを付加するか、情報自体をそのままにしてこれを暗号化したハッシュトータル値を付加するか、デジタル署名 (認証コード) を行なうかなどのいずれか、または複数を行なうようにしてもよい。

【0103】また情報にはソフトウェアプログラムも含まれ、これらの情報を格納した記録媒体を販売又はレンタルする際、前記キー格納部材を同梱して配布し、そのキー格納部材に格納されているキーによって情報の暗号化処理がなされ、キー格納部材が情報の利用には不可欠のようにすることにより、ソフトウェアを含む情報の不正コピーを防止することができる。

【0104】さらに情報がコンピュータネットワークなどによって送信されて販売又はレンタルされる場合には、該情報を暗号化した際のキー、ないしは該キーを暗号化した暗号化キーを格納したキー格納部材を別送し、これを用いて、受信は情報を復号化し、利用できるようにする。

【0105】

【発明の効果】本発明は前述のような構成になっており、情報の暗号化は同一 (共通) の値 (内容) の共通キー R を使用しているから、情報に対しては共通キー R のみで様に生産すればよいから処理が簡便である。

【0106】また、情報の利用者ごとに異なる値 (内容) のワークキー (R) Si を配布しているから、その解読は非常に困難である。

【0107】さらに情報の配布側と利用者側との間は、暗号化された情報 (I) R とワークキー (R) Si しか流れないので、機密は高度に保たれるなどの特長を有している。

【図面の簡単な説明】

【図 1】本発明の実施例に係る情報の受渡しシステムを説明するための構成例を示すブロック図である。

【図 2】その情報の受渡しシステムの流れを説明するための図である。

【図 3】その情報の受渡しシステムの他の流れを説明するための図である。

【図 4】その情報の受渡しシステムの他の流れを説明す

るための図である。

【図 5】その情報の受渡しシステムの他の流れを説明するための図である。

【図 6】その情報の受渡しシステムの他の流れを説明するための図である。

【図 7】その情報の受渡しシステムの他の流れを説明するための図である。

【図 8】その情報の受渡しシステムの他の流れを説明するための図である。

【図 9】パソコンに暗号処理装置を接続した状態を示す側面図である。

【図 10】その暗号処理装置の動作を説明するためのフローチャートである。

【図 11】暗号処理装置の変形例を示すブロック図である。

【図 12】暗号処理装置を内蔵したアダプタの斜視図である。

【図 13】暗号処理装置を内蔵した他のアダプタの斜視図である。

【図 14】暗号処理装置の変形例を説明するための図である。

【図 15】暗号処理装置のさらに他の変形例を説明するための図である。

【符号の説明】

1 暗号処理装置

3 暗号論理手段

4 暗号処理装置

5 キー格納手段

7 セキュリティ処理手段

8 キー照合手段

9 通信手段

10 情報 I (1)

14 情報 I (2)

20 アダプタ

20b 着脱部材

21 情報記録媒体

22 ネットワークシステム

24 スロット

25 入出力装置

30 パソコン

40 カード本体

41 サブカード

45、46 インターフェース

47 着脱部材

R 共通キー

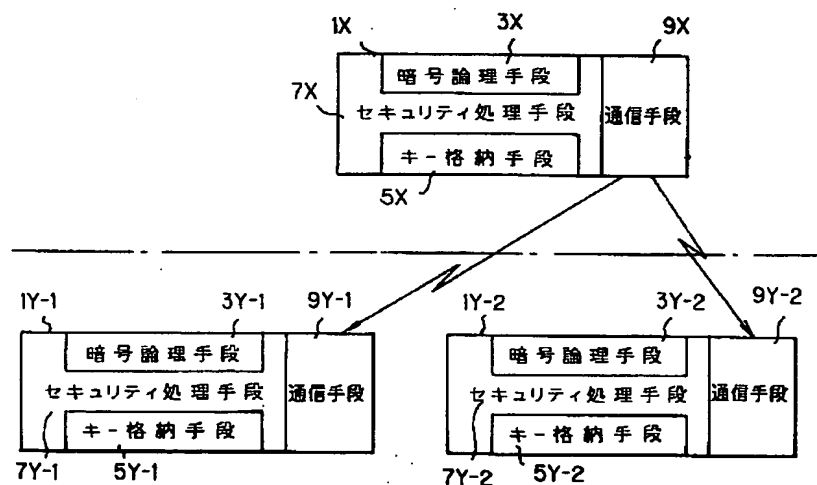
Si 個別キー

(R) Si ワークキー

I (1) オリジナル情報

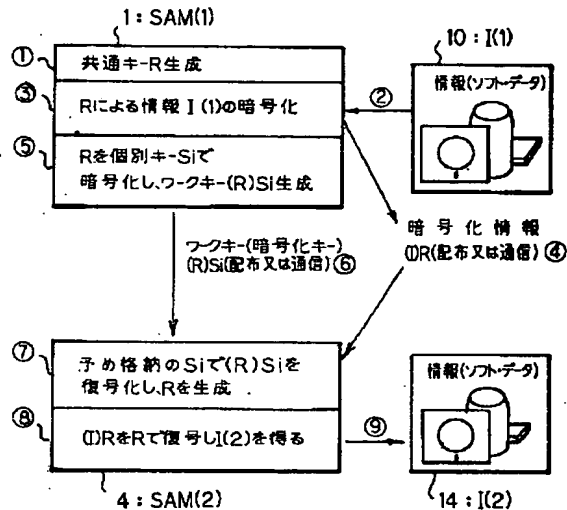
(I) R 暗号化情報

【図 1】



【図 2】

【図 2】



【図 4】

【図 4】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ① 共通キ-Rを生成。 ② 共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ オリジナル情報I(1)を共通キ-Rで暗号化して、暗号化情報IRを生成。 ④ ワークキ-(R)Si-A、(R)Si-Bと暗号化情報IRを、SAM(2)-A、SAM(2)-Bに、それぞれ送る。	⑥ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑧ 暗号化情報IRを共通キ-Rで復号化して、情報I(2)を生成。	⑥ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑧ 暗号化情報IRを共通キ-Rで復号化して、情報I(2)を生成。

【図 3】

【図 3】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ① 共通キ-Rを生成。 ② 共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ ワークキ-(R)Si-AをSAM(2)-Aに、(R)Si-BをSAM(2)-Bにそれぞれ送る。 ⑤ オリジナル情報I(1)を共通キ-Rで暗号化して、暗号化情報IRを生成。 ⑥ 暗号化情報IRをSAM(2)-A、SAM(2)-Bに、それぞれ送る。	④ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑦ 暗号化情報IRを共通キ-Rで復号化して、情報I(2)を生成。	④ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑦ 暗号化情報IRを共通キ-Rで復号化して、情報I(2)を生成。

【図 7】

【図 7】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ① 共通キ-Rを生成。 ② 共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ ワークキ-(R)Si-A、(R)Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。 ⑥ 暗号化情報IR-Aを共通キ-Rで復号化して、情報I(2)-Aを生成。	④ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑤ オリジナル情報I(1)-Aを共通キ-Rで暗号化して、暗号化情報IR-AをSAM(1)とSAM(2)-Bへ送る。	④ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑥ 暗号化情報IR-Bを共通キ-Rで復号化して、情報I(2)-Bを生成。

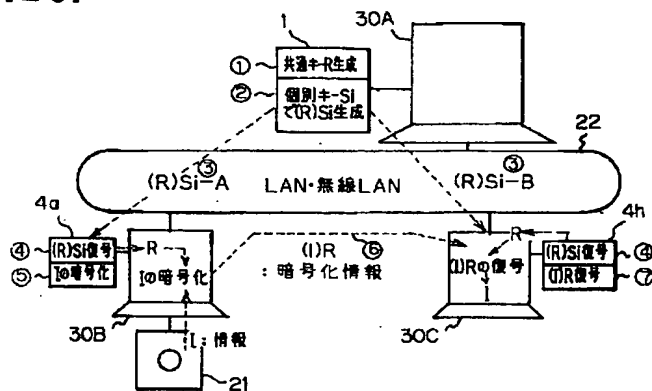
【図 5】

【図 5】

SAM(1)	SAM(2)-A	SAM(2)-B
① 共通キ-Rを生成。 ② SAM(2)-A用、SAM(2)-B用の個別キ-Si-A、Si-Bを生成。 ③ 個別キ-Si-A、Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。 ⑤ 共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ⑥ ワークキ-(R)Si-A、(R)Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。 ⑧ オリジナル情報I(1)を共通キ-Rで暗号化して、暗号化情報I(1)Rを生成して、SAM(2)-A、SAM(2)-Bへ、それぞれ送る。	④ 個別キ-Si-Aを格納。 ⑦ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑨ 暗号化情報I(1)Rを共通キ-Rで復号化して、情報I(2)を生成。	④ 個別キ-Si-Bを格納。 ⑦ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑨ 暗号化情報I(1)Rを共通キ-Rで復号化して、情報I(2)を生成。

【図 8】

【図 8】



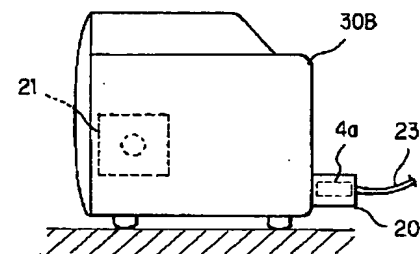
【図 6】

【図 6】

SAM(1)	SAM(2)-A	SAM(2)-B
① 個別キ-Si-A、Si-Bを生成、保有。 ② 共通キ-Rを生成。 ③ 共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ⑤ ワークキ-(R)Si-A、(R)Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。 ⑧ 暗号化情報I(1)R-Aを共通キ-Rで復号化して、情報I(2)-Aを生成。 ⑩ 暗号化情報I(1)R-Bを共通キ-Rで復号化して、情報I(2)-Bを生成。	④ 個別キ-Si-Aを付与、保有。 ⑦ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑨ オリジナル情報I(1)-Aを共通キ-Rで暗号化して、暗号化情報I(1)R-AをSAM(1)へ送る。	④ 個別キ-Si-Bを付与、保有。 ⑦ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑨ オリジナル情報I(1)-Bを共通キ-Rで暗号化して、暗号化情報I(1)R-BをSAM(1)へ送る。

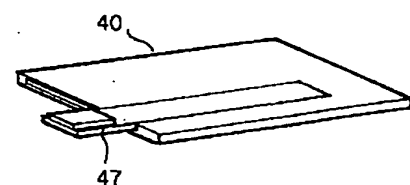
【図 9】

【図 9】



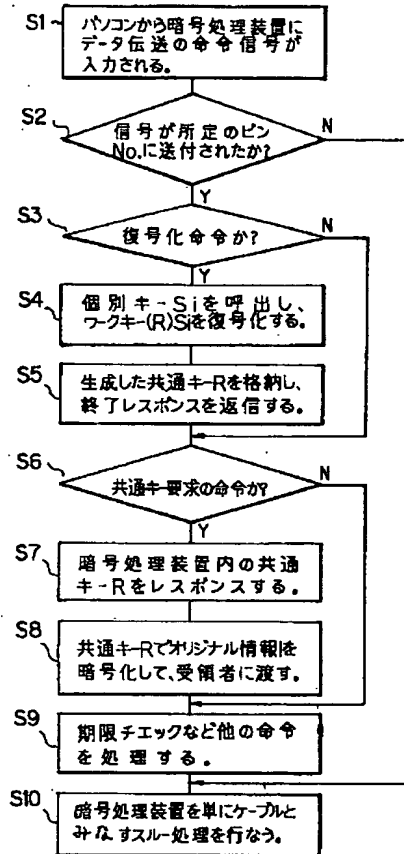
【図 15】

【図 15】



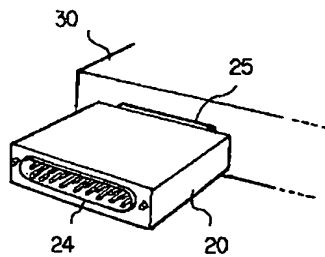
【図 10】

【図 10】



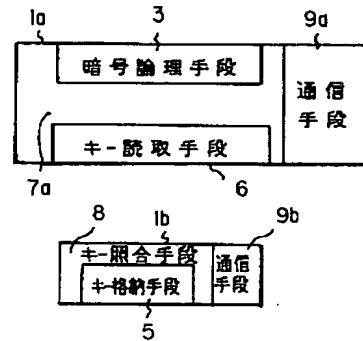
【図 12】

【図 12】



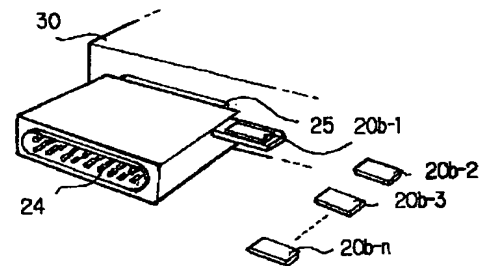
【図 11】

【図 11】



【図 13】

【図 13】



【図 14】

【図 14】

